



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/736,717	12/12/2000	David Michael Kurn	20206-036 (P00-3418)	8320

7590 09/26/2005

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

JACKSON, JENISE E

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 09/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/736,717

Applicant(s)

KURN ET AL.

Examiner

Jenise E. Jackson

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 July 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7 and 9-20 is/are rejected.
- 7) ☒ Claim(s) 8, 21 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 13-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The Applicant added new claims, but the Examiner cannot find in the specification the claim limitations described. Therefore, the claims 13-20 are rejected under 112^{1st}.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-7, 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot(6,317,829) in view of Eastlake.
5. As per claim 1, Van Oorschot discloses a cryptographic keys used during operation of a computer system(see col. 3, lines 20-24), providing an old set of cryptographic keys(see col. 6, lines 21-32, col. 7, lines 3-14); including at least a first cryptographic key protects an integrity of

Art Unit: 2131

secret information stored in a database(see col. 6, lines 33-47), and the second cryptographic key protects access to the secret information stored in the database(see col. 4, lines 52-58, col. 7, lines 30-41), checking with a key repository to determine if a certificate re-issuance is necessary, meanwhile maintaining the availability of the old set of cryptographic keys(see col. 6, lines 22-32, col. 7, lines 3-14); the new keys are stored in the database(see col. 4, lines 24-48, col. 7, lines 6-11), providing the new or revised keys to applications that need them when next requested by such applications(see col. 3, lines 30-39, col. 6, lines 22-32). Van Oorschot discloses an application, because the primary computing unit, and the server communicated the key history information via a internet link(see col. 5, lines 3-6), an application is inherent in Van Oorschot, because Van Oorschot discloses communicating the key information to the primary computing device via an Internet link, this link has an application, such as a web browser. However, Van Oorschot does not disclose key rollover. Eastlake does disclose key rollover.

6. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Van Oorschot with Eastlake to include key rollover, one would have been motivated to include key rollover of Eastlake, because in order to obtain high levels of security, keys must be periodically changed, or “rolled over”(see pg. 3 of Eastlake). Rollover is necessary because the longer a private key is used the more likely it is to be compromised due to cryptanalysis, accident or treachery(see pg. 3 of Eastlake).

7. As per claim 2, Van Oorschot discloses key repository utilizing one or more services of a specialized application acting as an extension of the key repository (col. 3, lines 27-39, col. 6, lines 22-32).

Art Unit: 2131

8. As per claim 3, Van Oorschot discloses the key repository utilizes the one or more services of the specialized application, authenticating authorization of the specialized application to perform one or more services(see col. 3, lines 27-39, 51-67, col. 7, lines 30-53).

9. As per claim 4, Van Oorschot discloses a command that when the key is about to approach expiration, a new key is issued(see col. 6, lines 22-32). Van Oorschot does not disclose invoking the command. Eastlake discloses invoking a key rollover. The motivation to include invoking the key rollover, is that being invoked as a result of a command, is the longer a private key is used, the more likely it is to be compromised due to cryptanalysis, accident or treachery(see pg. 3 of Eastlake).

10. As per claim 5, Van Oorschot discloses a periodic check which senses that the old set of cryptographic keys are approaching expiration (see col. 4, lines 24-47, col. 6, lines 21-32).

11. As per claim 6, Van Oorschot discloses a result of sensing an expired key(see col. 4, lines 24-47, col. 6, lines 21-32).

12. As per claim 7, Van Oorschot discloses wherein the applications are notified of the presence of new keys by the key repository process(see col. 8, lines 41-56).

13. As per claim 9, Van Oorschot discloses wherein the key repository process is prompted by the applications to invoke the method as a result of the applications detecting a key approaching expiration (see col. 6, lines 62-67, col. 7, lines 1-11).

14. As per claim 10, Van Oorschot discloses wherein the applications request the key repository process to provide a new key as a result of applications detecting an expired key(see col. 7, lines 1-14).

Art Unit: 2131

15. As per claim 11, Van Oorschoot discloses a key repository configured to maintain at least a first key and second key(see fig. 1, sheet 1), and a database coupled to the key repository(see fig. 1, sheet 1), and storing secret information wherein the first key protects an integrity of the secret information stored in the database(see col. 6, lines 33-49), and the second key protects access to the secret information stored in the database(see col. 4, lines 52-58, col. 7, lines 30-41).

16. As per claim 12, Van Oorschoot discloses at least one application that can access the key repository, wherein the at least one application is preauthorized to access the second key and can perform at least one function using the secret information without user intervention(see col. 5, lines 64-67, col. 6, lines 1-7).

17. Claims 8, and 21 are rejected under 112, but are allowable for the feature of an application detecting a missing key, and check with the key repository for that key and, if the missing key has been reissued, the applications receive a newly-issued key, the prior art of digital certificates and revocations, discloses that if a key is missing or lost, that the key can be recovered through various cryptographic techniques. In prior art it does not disclose that if a key is missing, reissuing another key.

18. Claims 13-20 are rejected under 112 1st, because the claimed limitations are not described in the specification.

Response to Amendment

19. The Applicant states that Van Oorschot, prior art that was applied to reject claims, does not disclose a first cryptographic key that protects integrity of secret information stored in a database and a second cryptographic key that protects access to the secret information stored in

Art Unit: 2131

the database. Further, the Applicant states that the second cryptographic key with a password taught in Van Oorschot is not a cryptographic key. The Examiner disagrees with the Applicant.

20. First, Van Oorschot does disclose a first cryptographic key that protects integrity of secret information stored in a database, because Van Oorschot discloses to help prevent unauthorized acquisition of the secret decryption keys, the public repository(i.e. database) includes a decryption private key encryptor for protecting sensitive data, thus this is a cryptographic key(see col. 6, lines 33-49). Second, the Examiner view the second cryptographic key as a password(see col. 7, lines 30-52), if the Applicant wishes to define or claim a more specific key the Applicant is urged to do so.

21. As per claims 8, and 21, previously indicated as allowable, thus Applicant arguments are moot. 112 1st rejection has been withdrawn, because Applicant has amended the specification to include the limitations of claims 8 and 21.

22. The Examiner also rejected claims 13-20 under 112 1st. The Applicant provided citations in the specification where the claim limitations were found. However, the Examiner still does not see how claims 17-18 are taught in the specification. The Examiner read the citations provided, but still does not see the claim limitations taught. Therefore, the rejection under 112 1st still stands.

Final Action

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2131

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

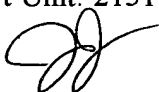
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 09/736,717

Art Unit: 2131



September 19, 2005

Page 8

CEL
Primary Examiner
AO2131
9/22/05